

**Directions:** Please complete shaded areas below.

**Department Name:** Enterprise Technology Services Department  
**Project Name:** ETSD Security Office Package  
**Project Amount:** \$258,000  
**Preparer Name & Contact Information:** Gary A. Gray, 305-275-7659

**Project Type:** Please check (✓) one.

☒ Enterprise    ☐ Communities of Interest    ☐ Department Specific

**Funding Source:** Please check (✓) one.

☒ GF Capital    ☐ Proprietary Capital

☐ **Mandated Requirement**  
(If checked (✓), please indicate who is mandating this request as well as the time frame)

☐ **Department Priority of Initiative (1, 2, 3, etc.)**

## Section A

### Background:

The ETSD Security Office is tasked with insuring the protection, stability, auditing and compliance of the county's IT resources. The various systems in place today need to be enhanced to continue to support the ability to protect our resources. Compliance regulations require more attention to be placed on the ability to track all access for auditing purposes such as HIPPA. In addition, due to the County's initiative to bring more of its resources and services to the citizen, there is an increased exposure from the Internet (Cyber Security). Requirements are also necessary to insure the use of newer technology is not inviting external forces to test the vulnerability of the County's resources. The demand for security review and investigation has led to a more proactive approach in our ability to secure the assets and resources of the County.

This business case supports the following security initiatives in order of priority:

- Internet Mail Gateway Protection - Upgrading the County's Internet E-mail Architecture from Servers to Appliances
- E-Mail SPAM Reduction - Reducing the amount of SPAM received in County E-Mails
- Network Intrusion Protection - Increasing the ability to identify and prevent network intrusions throughout the County's network
- Remote Access Protection - Enforcing the County's network security policies for remote access/users
- Wireless Access Protection - Enforcing the County's network security policies for wireless access/users

**Problem Statement:**

**Internet Mail Gateway Protection - Upgrading the County's Internet E-mail Architecture from Servers to Appliances**

Currently the architecture supporting Internet mail is based on NT Servers. We are processing over 1 million messages a day and the infrastructure cannot keep up and would require constant server upgrading. By procuring an appliance based solution, we will be able to insure the timely delivery of mail.

**E-Mail SPAM Reduction - Reducing the amount of SPAM received in County E-Mails**

Currently the software we use to prevent SPAM mail from entering our environment is adequate at best. Due to the rise in SPAM, the need to acquire better software has become apparent. By procuring a better software package we expect to be able to block 99.99% of SPAM.

**Network Intrusion Protection - Increasing the ability to identify and prevent network intrusions throughout the County's network (5 year plan)**

Currently there is no way of detecting malicious or virus based activity throughout the County's network. With the proper hardware in place to complement the county's Firewalls and anti-virus software systems, we will be able to protect the network against attacks "embedded" within what a firewall might perceive as normal network traffic. We will also be able to detect malicious code brought into the internal network by remote devices such as laptops by both county employees and vendors, which is one of the major problems the county faces today. We will also be able to reduce the amount of man-hours currently spent identifying, cleaning and restoring infected systems by isolating the incident to the area or department in which it was introduced and not allowing it to spread across the entire enterprise..

**Remote Access Protection - Enforcing the County's network security policies for remote access/users**

Currently there is no way of enforcing the County's network security policies for remote users. The ability to enforce our network security policies by isolating the connection and performing integrity will eliminate the current problem that the County faces in regards to virus and malicious code. A large portion of the viruses that enters the County's network is transmitted by remote workstations that are infected and are not being proactively protected. The successful enforcement will insure the workstations are protected and in turn will protect the County's network.

**Wireless Access Protection - Enforcing the County's network security policies for wireless access/users (5 year plan)**

Currently there is no way of enforcing the County's network security policies for wireless users. The ability to require user id/password authentication prior to accessing the network wirelessly will enforce our network security policies and will prevent unauthorized users from having access to the County's networks with no type of authentication taking place. This will protect the County's internal network and better secure our wireless infrastructure county wide.

**Solution:**

**Internet Mail Gateway Protection - Upgrading the County's Internet E-mail Architecture from Servers to Appliances**

Procure appliances to replace the current server based infrastructure at a cost of \$60,000.

**E-Mail SPAM Reduction - Reducing the amount of SPAM received in County E-Mails**

Procure software to reduce the percentage of SPAM received by county mail users at a cost of \$50,000.

**Network Intrusion Protection - Increasing the ability to identify and prevent network intrusions throughout the County's network (5 year plan)**

Launch initial implementation by procuring hardware to accomplish Intrusion protection of the County's gateway to the Internet at a cost of \$50,000.

**Remote Access Protection - Enforcing the County's network security policies for remote access/users**

Procure software to accomplish the enforcement of the County's network security policies for remote users at a cost of \$48,000.

**Wireless Access Protection - Enforcing the County's network security policies for wireless access/users (5 year plan)**

Launch initial implementation by procuring software to accomplish the enforcement of the County's network security policies for wireless users in test location at a cost of \$50,000.

**Expected Benefits / Direct Payback:**

All aspects of this request will benefit the county by reducing possible network downtime, reducing the County's exposure to Cyber Security and reducing the risk involved with new technologies.